TCP/IP

TCP/IP (Transmission Control Protocol/Internet Protocol, ou Protocolo de controle de Transmissão / Protocolo da Internet) se refere ao conjunto de protocolos utilizados na Internet. Ele inclui uma série de padrões que especificam como os computadores vão se comunicar e cria convenções para interconectar redes e para o routeamento através dessas conexões.

Os protocolos da Internet (IP) são o resultado de um projeto da DARPA (Defense Advanced Research Projects Agency, ou Agência de Projetos de Pesquisa Avançada de Defesa) sobre conectividade entre redes no final dos anos 70. Ele foi utilizado em todas as redes de longa distância do sistema de Defesa dos EUA em 1983, mas não foi amplamente aceito até ser incorporado ao BSD (Berkeley Software Distribution) Unix 4.2. A populariedade do TCP/IP é baseada em:

- Estrutura cliente-servidor robusta. O TCP/IP é uma excelente plataforma cliente-servidor, especialmente em ambientes WAN (wide-area network, ou redes de grande alcance).

- Compartilhamento de informações. Milhares de organizações miltiares, educacionais, científicas e comerciais compartilham dados, correio eletrônico (e-mail), e outros serviços na Internet usando o TCP/IP.

- Ampla disponibilidade. Implementações do TCP/IP estão disponívies em praticamente todos os sistemas operacionais populares. Seu código fonte é amplamente disponível em várias implementações. Fabricantes de bridges, routers e analizadores de redes oferecem suporte para o TCP/IP em seus produtos.

Existem alguns conceitos básicos que são imprencindíveis ao entendimento do TCP/IP e de redes que o utilizam.

Existem algumas analogias entre computadores e telefones e o número de IP é uma delas. Você pode imaginar o número IP como um número de telefone com todos os códigos de discagem internacional. Isto significa que qualquer máquina pode contactar outra máquina usando o número de IP, bastando apenas que exista um caminho entre as 2 máquinas. Além disso toda máquina na rede tem de ter um nº de IP.

Isto também significa que 2 máquinas na mesma rede NÃO podem ter o mesmo número de IP. Essa restrição só ocorre para máquinas na mesma rede, pois máquinas numa rede não conectada usualmente tem número de IP iguais, por algumas razões técnicas. No caso da analogia com os telefones, imagine 2 pessoas morando em países diferentes que possuam o mesmo número de telefone (apenas os números locais). Nesse caso não há conflito (exceto talvez na sua mente!

O número de IP tem 4 bytes de tamanho e tem um formato específico, xxx.xxx.xxx.xxx (exemplo : 200.241.216.20). Isso significa que cada grupamento xxx só pode ir de 0 à 255 (pois essa é a capacidade de 1 byte).

Existem 3 classes de endereços IP : classes A, B, C. A diferença entre as classes é a forma de como o nº de IP é interpretado. O nº de IP é divido em duas partes : o endereço da rede e o enderço da sub-rede. Considere o nº IP da seguinte forma : w.x.y.z (ex: 200.241.216.20)

Classe	Nº	Indicador	Indicador da	Nº de redes	Nº de sub-redes

	de IP	da rede	Sub-rede	disponíveis	disponíveis
A	1.126	w	x.y.z	126	16,777,214
B	128.191	w.x	y.z	16,384	65,534
C	192.223	w.x.y	z	2,097,151	254

Obs: O endereço 192.168 é reservado para uso em redes internas, o endereço 127 é utilizado para testes de loopback e os acima de 224 (inclusive) são reservados para protocolos especiais.

Uma sub-rede é uma rede ligada diretamente a Internet através de uma rede pertencente a Internet. A rede pertencente recebe um nº de IP, e distribui nº de IP dentro de sua sub-rede. As classes apenas definem quantas sub-redes um nº de IP tem. De acordo com a tabela, existem 126 nº de IP da classe A e cada um deles pode ter 16.777.214 sub-redes. Você logo pode imaginar que não existem endereços classe A para todo mundo, e tem razão, atualmente não existem endereços classe A e B disponíveis na Internet, e os de classe C estão acabando, o IETF (Internet Engenniering Task Force, ou Força Tarefa de Engenharia da Internet) está estudando a expansão desses números.

As máscaras de sub-rede identificam a classe do nº de IP. A primeira vista isso parece desnecessário, pois basta olhar o primeiro número do nº do IP para determinar sua classe. Mas acontece que um nº de IP classe A pode funcionar como um classe B ou classe C, dependendo da estrutura interna de sua sub-rede. Um exemplo : Imagine uma empresa com 200 filiais no Brasil conectadas por uma rede própria. A matriz tem um nº de IP classe A, digamos 100 e distribui suas sub-redes da seguinte forma :

100.1.0.0	Matriz
100.2.0.0	Filial 1
100.3.0.0	Filial 2
100.201.0.0	Filial 200

Para as filiais, o nº de IP (ex: 100.201.0.0) é de classe B, pois só tem 16.384 sub-redes disponíveis, embora comece com 100. Dentro das filiais ainda é possível se distribuir sub-redes, as quais teriam nº de IP classe C.

Para que o roteamento funcione corretamente, os computadores precisam saber qual a classe do nº de IP, e elas são as seguintes:

Classe	Máscara de Sub-rede
A	255.0.0.0
B	255.255.0.0
C	255.255.255.0

O gateway padrão é a máquina para quem pedimos ajuda quando não conseguimos achar uma outra máquina na rede. Funciona assim: Quando uma máquina na rede precisa se comunicar com uma outra, ela emite um pedido de conexão (esse pedido é feito através de broadcasting, ou seja, a máquina envia um pedido a toda a rede, e apenas a máquina destino responde) e aguarda uma resposta. Se a resposta não vier, ela

entra em contato com o gateway padrão e solicita que o mesmo conecte com a máquina destino. Se o gateway conseguir se conectar à máquina destino, ele fica como "intermediador" dessa conexão, caso contrário ele avisa a máquina solicitante que não foi possível encontrar a máquina destino.

Essa estrutura de procura visa diminuir o tráfego desnecessário na rede. Imagine só se toda a solicitação de conexão realizada na Internet (e em todas as redes conectadas à Intenet) fosse enviada para todos os computadores ligados à ela! Seria um tráfego muito grande. Ao invés disso, o broadcasting é feito em níveis, primeiro na LAN (local area network, ou rede local), depois na WAN de sua cidade ou estado, depois na WAN nacional até chegar na WAN internacional. Reduz-se desse modo todo o tráfego interno às WANs e LANs, aliviando as linhas de conexão.

Essas 3 letras não significam muita coisa para a maior parte das pessoas, mas elas significam Domain Name System (ou Sistema de Nomes de Domínio). Essas 3 palavras também não significam muita coisa para a maior parte das pessoas também, por isso vamos à analogia com o telefone. Quando deseja telefonar para a loja da esquina, você consulta o catálogo, descobre o telefone de lá e liga. Você não consegue telefonar para lugar algum se não souber o número do telefone. Na rede TCP/IP acontece a mesma coisa. Os usuários não decoram o número IP das máquinas, e sim seus nomes. Mas para se alcançar uma máquina na rede, precisamos do seu número de IP. Para resolver isso, foi criado o DNS, um serviço diponível na rede que, dado um nome de máquina, ele retorna o número de IP da mesma.

Existe uma particularidade aqui. No caso da rede local estar conectada a alguma outra, é recomendável que o servidor DNS (o programa que oferece o serviço DNS) seja executado na máquina de ligação entre as 2 redes (o gateway), para que no caso do nome requisitado não existir na rede local, o DNS possa pedir ao servidor DNS da outra rede para pesquisar tal nome.

O Windows NT oferece um serviço semelhante, o WINS (Windows Internet Name System, ou Sistema de nomes da Internet do Windows). A principal diferença entre os dois é que o DNS usa uma tabela estática, e o WINS usa uma tabela dinâmica. No caso do servidor DNS rodar numa máquina Windows NT é recomendável que ele seja substituído pelo WINS.

Mais um caso de 4 letras que não significam nada para a maioria das pessoas. Mas infelizmente não existe uma boa analogia para o DHCP, portanto vamos direto ao assunto: DHCP significa Dynamic Host Configuration Protocol ou seja : Protocolo de Configuração de Host Dinâmico. Numa rede TCP/IP, todo computador tem de ter um número de IP distinto. Isto significa que antes de colocar uma nova máquina na rede, o administrador teria de checar quais números estão sendo utilizados para poder escolher um nº adequado para a nova máquina. Em pequenas redes isso é possível de ser feito, mas em grandes redes isso se torna uma tarefa muito tediosa e sujeita a falhas. Para evitar isso, foi criado o DHCP. Quando uma máquina entra na rede, ela procura o servidor DHCP (cujo nº de IP foi previamente fornecido) e solicita um nº de IP para si própria. O servidor verifica qual o nº disponível, informa ao solicitante esse nº e o torna indisponível para futuras solicitações. Dessa maneira, a administração dos nº de IP é feita automaticamente e não existem problemas de conflito. Quando a máquina solicitante sai da rede, o servidor DHCP torna seu nº de IP disponível novamente.

Uma porta pode ser vista como um canal de comunicações para uma máquina. Pacotes de informações chegando a uma máquina não são apenas endereçadas à maquina, e sim à máquina numa determinada porta. Você pode imaginar uma porta como sendo um canal de rádio, com a diferença fundamental de que um computador pode "ouvir" a todos os 65000 canais possíveis ao mesmo tempo!

Entretanto, um computador geralmente não está escutando a todas as portas, ele escuta umas poucas portas específicas. E ele não vai responder a um pedido que chegue numa porta a qual ele não esteja escutando.

Existem uma série de portas pré-definidas para certos serviços que são aceitos universalmente. As principais são :

Serviço	Porta	Descrição
FTP	21	File Transfer Protocol (Protocolo de Transferência de Arquivos)
Telnet	23	Para se conectar remotamente a um servidor
SMTP	25	Para enviar um e-mail
Gopher	70	Browser baseado em modo texto
HTTP	80	Protocolo WWW - Netscape, Mosaic
POP3	110	Para receber e-mail
NNTP	119	Newsgroups
IRC	6667	Internet Relay Chat - Bate papo on-line
Compuserve	4144	Compuserve WinCIM
AOL	5190	America Online
MSN	569	Microsoft Network

- **Roteador** : É um computador especial que é utilizado para conectar 2 ou mais redes distintas. Ele tem esse nome porque tem de "rotear" (ou redirecionar) os pacotes de uma rede para outra, atuando como um "guarda de trânsito" para os pacotes entre as redes.

- **Gateway** : O gateway é um computador que também é utilizado para conectar 2 ou mais redes distintas. A principal diferença para o roteador é que o gateway não tem hardware especial para efetuar o roteamento. Usualmente os gateways conectam LANs e os roteadores, WANs. Em vários casos se utiliza um roteador em conjunto com um gateway.

Uma rede utilizando o TCP/IP tem uma estrutura básica composta por um (ou mais) servidor rodando um servidor DNS (ou WINS), DHCP, SMTP, POP3 e os servidores dos serviços desejados (HTTP, Gopher, Telnet e etc) e as máquinas clientes solicitando esses serviços. Para se interligar essa rede a uma outra rede TCP/IP, se faz necessário o uso de um roteador ou gateway e da correta configuração da rede. Existem 2 maneiras de se ligar a LAN à Internet :

- Atribuindo-se um nº de IP válido para cada máquina na rede, o que pode ser impossível para redes com muitas máquinas.

- Atribuindo-se um nº de IP válido para o gateway e utilizando-se o nº de IP 192.168.x.x internamente.

Como o segundo caso é o mais factível, vamos observá-lo melhor. Nele, se utiliza internamente à LAN o IP 192.168.x.x, que quando da determinação do padrão dos nº de IP foi reservado para uso em redes internas, ou seja, nenhuma máquina ligada diretamente à Internet tem um IP 192.168.x.x. Isso é necessário pois como já vimos nenhuma máquina pode ter um nº de IP que já esteja sendo utilizado por uma outra máquina.

O gateway tem 2 interfaces de rede, uma para se conectar à Internet e outra para se conectar à LAN. À interface da Internet é atribuido o nº de IP válido na Internet e na da LAN o nº de IP do tipo 192.168.x.x (usualmente 192.168.0.1). Nas máquinas da LAN o nº de IP é do tipo 192.168.x.x (aonde o 1º "x" é o mesmo do do gateway) e o gateway default é o IP do gateway voltado para a LAN (192.168.x.x). Dessa forma podemos ter até 16.384 máquinas na internet por nº de IP válido. Essa estrutura também facilita a adoção de medidas de segurança contra intrusos da Internet, pois como todo o tráfego Internet passa pelo gateway, basta protegê-lo para proteger toda a LAN.

TCP e IP

O TCP e o IP são apenas 2 membros da família TCP/IP. IP é um protocolo que providência a entrega de pacotes para todos os outros protocolos da família TCP/IP. O IP oferece um sistema de entrega de dados sem conexão. Isto é, os pacotes IP não são garantidos de chegarem ao seu destino, nem de serem recebidos na ordem em que foram enviados. O checksum do IP confirma apenas a integridade do cabeçalho do pacote. Desta maneira, a responsabilidade pelos dados contidos no pacote do IP (e sua sequência) é tarefa de protocolos de mais alto-nível.

Talvez o protocolo de alto nível do IP mais comum seja o TCP. O TCP oferece um confiável protocolo baseado em conexão encapsulado no IP. O TCP garante a entrega dos pacotes, assegura o sequenciamento dos pacotes, e providencia um checksum que valida tanto o cabeçalho quanto os dados do pacote. No caso da rede perder ou corromper um pacote TCP/IP durante a transmissão, é tarefa do TCP retransmitir o pacote faltoso ou incorreto. Essa confiabilidade torna o TCP/IP o protocolo escolhido para transmissões baseadas em sessão, aplicativos cliente-servidor e serviços críticos como correio eletrônico.

Porém essa confiabilidade tem um preço. Os cabeçalhos dos pacotes TCP requerem o uso de bits adicionais para assegurar o correto sequenciamento da informação, bem como um checksum obrigatório para garantir a integridade do cabeçalho e dos dados. Para garantir a entrega dos pacotes, o protocolo também requer que o destinatário informe o recebimento do pacote.

Tal "informação de recebimento" (ou ACKs, de acknowledgments) geram tráfego adicional na rede, diminuindo a taxa de transferência de dados em favor da confiabilidade. Para reduzir o impacto na peformance, a maioria dos servidores enviam um ACK para todo segmento de dados (ao invés de todo pacote) ou quando um ACK expira.

UDP

Se a confiabilidade não é essencial, o UDP (User Datagram Protocol), um complemento do TCP, oferece um serviço de transmissão de dados sem conexão que não garante nem a entrega nem a correta sequência dos pacotes enviados (bem parecido com o IP). Checksums no UDP são opcionais, ofereccndo assim uma maneira de se trocar dados em uma rede altamente confiável sem consumir desnecessariamente recursos da rede.

ARP e ICMP

Dois outros protocolos na família TCP/IP tem importantes funções, embora essas funções não estejam diretamente relacionadas com a transmissão de dados: ARP (Address Resolution Protocol, ou Protocolo de Resolução de endereços) e ICMP (Internet Control Message Protocol, ou Protocolo de Controle de Mensagens da Internet). O ARP e o ICMP são protocolos de manutenção que mantêm a estrutura do IP e usualmente são invisíveis aos usuários e às aplicações.

Os cabeçalhos do IP contém tanto o endereço IP da origem quanto do destino, mas o endereço do hardware também tem de ser conhecido. O IP obtém um endereço de hardware de um determinado sistema difundindo pela rede um pacote especial de requisição (um pacote ARP de requisição) contendo o endereço IP do sistema com o qual está tentando se comunicar. Todos os nós da rede local que tiverem o ARP habilitado detectam essa difusão, e o sistema que tem o número de IP em questão envia um pacote (do tipo ARP reply, ou resposta ARP) contendo seu endereço de hardware para o computador que o solicitou. O endereço de hardware e o endereço IP do computador estão é armazenado no cache do ARP para uso futuro. Como a resposta ARP também é feita na forma de difusão, é normal que outros nós usem essa informação para atualizar seus caches ARP.

- ICMP permite que 2 nós em uma rede IP compartilhem o status do IP (protocolo) e informação de erros. Esta informação pode ser usada por protocolos de alto nível para tratar problemas de transmissão ou para administradores de rede para detectar problemas na rede. Embora estejam encapsulados em pacotes IP, o ICMP não é considerado um protocolo de alto nível (ele é necessário em toda implementação do TCP/IP). O utilitário ping faz uso do ICMP para determinar se um certo endereço IP na rede está operacional. Isto é útil para diagnosticar problemas em redes IP ou falhas em gateways.

- **Outros Protocolos**

Além desses protocolos citados, existem os protocolos de alto-nível, como o Telnet, FTP, HTTP e etc. Vamos a uma breve descrição deles :

- **Telnet** : É um protocolo que permite o logon em máquinas remotas. Você passa a utilizar a máquina remota para realizar o processamento. No Windows NT existe o RAS (Remote Access Service, Serviço de Acesso Remoto) que tem os mesmos objetivos do Telnet.

- **FTP** : File Transfer Protocol (protocolo de transferência de arquivos), como o nome já diz é utilizado para a transferência de arquivos.

- **HTTP**: Hyper Text Transfer Protocol : É o protocolo utilizado pela Web, ele transmite textos, gráficos e qualquer outro tipo de arquivo (substituindo o FTP) além de permitir a navegação através de hiper texto.